IBM Watson Health Core

ご利用条件 (以下「ToU」といいます。) は、本「IBM ご利用条件 – SaaS 特定オファリング条件」(以下「SaaS 特定オファリング条件」といいます。)、および以下の Web サイトでご覧いただける「IBM ご利用条件 – 一般条件」(以下「一般条件」といいます。) で構成されています (URL:http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/)。

「SaaS 特定オファリング条件」と「一般条件」の規定に矛盾がある場合、「SaaS 特定オファリング条件」が優先して適用されるものとします。「IBM SaaS」の注文、そのアクセスまたは利用により、お客様は「ToU」に同意したものとみなされます。

「ToU」には、「IBM パスポート・アドバンテージのご契約条件」、「IBM パスポート・アドバンテージ・エクスプレスのご契約条件」、または「IBM SaaS 特定オファリングのご契約条件」のうち該当する契約条件 (以下「本契約」といいます。) が適用され、これらと「ToU」を合わせて完全な合意として成立します。

1. IBM SaaS

以下の「IBM SaaS」オファリングに、これらの「SaaS 特定オファリング条件」が適用されます。

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. 課金単位

「IBM SaaS」は、「取引文書」で規定された以下の課金単位のいずれかに従って販売されます。

a. **「アクセス」**は、「IBM SaaS」を取得する際の課金単位です。「アクセス」とは、「IBM SaaS」を利用する権利です。お客様は、お客様の「証書 (PoE)」または「取引文書」に定める課金期間中に、「IBM SaaS」を利用するために 1 件の「アクセス」使用許諾を取得しなければならないものとします。

b. **「個体」**は、「IBM SaaS」を取得する際の課金単位です。「個体」は 1 つの物または 1 人の人です。お客様は、お客様の「PoE」または「取引文書」に定める課金期間中に「IBM SaaS」が処理または管理する「個体」をカバーするのに十分な使用許諾を取得しなければならないものとします。

本「IBM SaaS」において、「個体」には、そのデータが「IBM SaaS」で管理される人、デバイスまたはモバイル・アプリケーションが含まれます。

c. **「インスタンス」**は、「IBM SaaS」を取得する際の課金単位です。「インスタンス」とは、「IBM SaaS」の特定の構成へのアクセスを意味します。お客様の「PoE」または「取引文書」に定める課金期間中にアクセスおよび使用が可能となる「IBM SaaS」の各「インスタンス」のために十分な使用許諾を取得しなければならないものとします。

3. 料金および課金

「IBM SaaS」に対する料金は、「取引文書」に記載されます。

3.1 1 か月に満たない期間の料金

「取引文書」に記載された 1 か月に満たない期間の料金は、按分にて算定される場合があります。

3.2 超過料金

課金期間中のお客様の「IBM SaaS」の実際の利用が、「PoE」に記載される使用許諾範囲を超える場合には、お客様は、「取引文書」の規定に従い、その超過分について請求されます。

4. 期間および更新オプション

「IBM SaaS」の期間は、「注文関連文書」に記述されるとおり、「IBM SaaS」の「パイロット」稼働環境へのお客様のアクセスについて、IBM がお客様に通知した日に開始します。「個体」の使用許諾のサブスクリプション期間は、「実稼働」稼働環境へのお客様のアクセスについて IBM が通知した日に開始

します。「注文関連文書」には、「IBM SaaS」が自動的に更新されるか、継続利用ベースで続行されるか、期間満了時に終了するかが記載されます。

自動更新の場合には、お客様が期間満了日の少なくとも 90 日前までに書面により更新しないことを通知する場合を除き、「IBM SaaS」は、「PoE」に定める期間につき自動更新されます。

継続利用の場合は、「IBM SaaS」は、お客様が 90 日前までに書面により終了を通知するまで、月単位で継続利用することができます。「IBM SaaS」は、かかる 90 日の期間後の暦月末日まで引き続き利用することができます。

5. テクニカル・サポート

IBM は、テクニカル・サポートの連絡先情報、保守時間、その他情報およびプロセスを規定する IBM Software as a Service Support Handbook を提供します。テクニカル・サポートの連絡先情報およびサポート運用に関するその他の詳細は、IBM SaaS Support Handbook (https://support.ibmcloud.com) でご確認いただけます。

「IBM SaaS」に関するテクニカル・サポートおよび単純な構成要求は、電子送信を通じて提供されます。テクニカル・サポートは「IBM SaaS」で提供されるものであり、個別のオファリングとして利用できるものではありません。

問題インシデントを報告する際、文書や情報には、「保護医療情報 (PHI)」や「機微な個人情報 (SPI)」を含む「個人情報 (PI)」を一切含めてはなりません。

6. 定義

「適用法」とは、法律、法規や制定法、規則、規制、命令、指令、法令や政府機関発行の要求、または一般に認識されている業界標準のうち、本 ToU の遂行に適用されるものをいいます

「API」とは、アプリケーション・プログラム・インターフェースのことで、ソフトウェア・アプリケーションを構築するためのルーチン、プロトコル、ツールのセットをいいます。API は、グラフィカル・ユーザー・インターフェース (GUI) コンポーネントをプログラムする際のソフトウェア・コンポーネントの対話方法や使用方法を指定します。

「権限を有する管理者」とは、プラットフォームの維持と信頼できる運用を管理する責任がある、お客様の従業員、承認されたお客様の請負業者、個人、またはグループをいいます。責任には、構成、サポート、ならびにユーザーおよびアカウントの管理が含まれる場合があります。当該管理者は、Watson Health システムについて調査をセットアップする責任のある臨床研究者である場合もあります。

「権限を有する個体」とは、認証された人、モバイル・アプリケーションまたはデバイスのうち、Watson Health Core へデータを送信するためのアクセス権へのアクセスを付与されたものをいいます。これには、お客様、調査参加者、顧客、またはお客様の患者が含まれる場合があります。

「お客様の適用可能なデータ法」とは、本契約、「関連文書」、ならびに両当事者間の適用可能な「サービス記述書」、「注文関連文書」および「作業指示書」に基づくお客様の義務の遂行に適用できる「データ法」をいいます。

「お客様データ」とは、お客様により、またはお客様のために、「IBM SaaS」に入力されたあらゆるデータをいいます。お客様自身のデータなのか、お客様の顧客または第三者により、またはそれらのために入力されたものかどうかは関係なく、また第三者の健康デバイスからのデータも含まれます。

「データ法」とは、データ保護、プライバシー、またはセキュリティーに関連する「適用法」をいいます。

「データ主体」とは、特定された個人または特定可能な個人で、「個人データ」が関連する者をいいます。

「指定データ・センター」とは、「取引文書」で 1 次災害復旧データ・センターに対応するものとして記載されたデータ・センターをいい、「IBM SaaS」についてお客様のインスタンスがある場合にはそれを実行します。

「ヘルス・データ」とは、イメージを含むデータまたは情報のうち、健康に関する「個人情報」をいいます。

「ヘルス・データ対応」とは、「IBM SaaS」に関して、「ヘルス・データ」の「対象管轄区」において適用されるセキュリティー標準およびプライバシー標準、法律、ならびに規制を満たす「IBM SaaS」の能力をいいます。これには、HIPAA (「HITECH 法」の修正が反映されたもの) を実施する規制をまとめた「パート 164 のサブパート A およびサブパート C」に規定された実装仕様、および「ヘルス・データ」に関するその他の「適用法」が含まれます。ただし、IBM が「ビジネス・アソシエート」または「データ・コントローラー」の資格で役割を果たすということではありません。

「HIPAA」とは、「米国における医療保険の相互運用性と説明責任に関する法律 (1996 年改訂)」をいいます。これには、「米国経済再生法 (2009 年制定)」の一部である「米国における経済および臨床上の健全性のための医療情報技術に関する法律」(以下「HITECH 法」といいます。)、「米国連邦規則集 (C.F.R.) 45 のパート 160 およびパート 164」に従って米国社会福祉保健省が HIPAA に基づき施行した特定の規制、ならびに「HITECH 法」に従って施行された特定の規制が含まれます。

「IBM の適用可能なデータ法」とは、本契約、「関連文書」、ならびに両当事者間の適用可能な「サービス記述書」、「注文関連文書」および「作業指示書」に基づく IBM の義務の遂行に適用できる「データ法」をいいます。

「IBM 担当者」とは、(a) IBM、その「関連会社」、およびその「従契約者」、ならびに上記のそれぞれに関して各自の従業員、ならびに (b) 第三者サプライヤーをいいます。いずれの場合も、本契約および該当する「関連文書」に従って IBM の代わりに、または IBM がその他の方法でお客様の「個人データ」にアクセスすることを許可した者に対して、サービスを遂行します。

「対象国」とは、28 の EU 加盟国およびスイス、ならびに IBM がこのリストに随時追加できる国をいいます。

「個人データ」または**「個人情報」**とは、電子記録および紙の記録を含むあらゆるメディアまたは形式の情報のうち、特定された個人または特定可能な個人に関連するもの、特に ID 番号、もしくはその人物の身体的、生理的、精神的、経済的、文化的もしくは社会的なアイデンティティーに固有の 1 つ以上の要因に言及することで、直接的または間接的に、特定される可能性のある者にあたる「特定可能な個人」に関連するものをいいます。

「プロセス」およびその変化形 (**プロセッシング**など) (定義語か否かは関係ありません。) は、自動手段によるか否かを問わず、データを用いて実行される、あらゆる運用または運用セットをいいます。ここでいう運用には、収集、記録、編成、保管、適応もしくは変更、取得、コンサルテーション、使用、送信による開示、伝播もしくはその他の方法での提供、調整もしくは組み合わせ、妨害、消去または消滅などがあります。

「処理済みデータ」とは、「ヘルス・データ」および「個人データ」を含む、あらゆるデータ、機密もしくは専有の情報または資料のうち、本契約、「関連文書」、ならびに「サービス記述書」、「注文関連文書」、および「作業記述書」、またはそのいずれかに準じて IBM が処理するものをいいます。

「セキュリティー・インシデント」は、SBCA に規定されている定義どおりです。

7. アカウント管理

「IBM SaaS」は、お客様の許可ユーザー (以下「**許可ユーザー**」または「**権限を有する管理者**」といいます。) にのみアクセスできます。お客様は、「IBM SaaS」にアクセスする権限を与えられたアカウント (これには、許可アプリケーション、お客様の担当者、お客様の第三者サービス・プロバイダーおよび請負業者が含まれる場合があります。) を制御します。また、(i) すべての許可ユーザーを制御すること (許可ユーザーの ID の確認が含まれますが、これに限定されません。)、および (ii) 許可ユーザーのみが「IBM SaaS」にアクセスすることを徹底させることに全責任を負います。

「権限を有する個体」のうち、お客様の顧客、患者または調査参加者は、「IBM SaaS」にデータをアップロードするという目的のためだけにアクセスを付与されなければなりません。この場合、かかる「権限を有する個体」は「IBM SaaS」へのその他のアクセスを一切有しません。

8. プライバシー

8.1 一般要件

両当事者間において、お客様は、お客様の「個人データ」のすべてについて唯一のコントローラーであり、またお客様は IBM をデータ・プロセッサーとして指名します。「適用可能なデータ法」に従い、お客様は、お客様の「個人データ」の IBM による処理に関連して IBM に指示を出す権利を有します。

IBM がお客様の「個人データ」を処理する限りにおいて、IBM は以下を行うものとします。

a. 「IBM の適用可能なデータ法」を遵守する。

b. お客様の「個人データ」とその他のソースからのデータを混合しない。ただし、以下のいずれかの場合は除きます。

- お客様からそうするよう具体的に指示されている場合を除き、「IBM SaaS」を提供するために必要な場合で、その他の目的のためではない場合。
- 本 ToU の条件および「SBCA 特則」に準じる場合。

IBM がお客様の「個人データ」を処理する限りにおいて、お客様は以下を行うものとします。

a. 「お客様の適用可能なデータ法」を遵守する。

b. お客様が、お客様の「関連会社」、患者、エンド・ユーザー、「データ主体」、およびその他のお客様の第三者と、またはそのいずれかと交わすすべてのコミュニケーションに対して責任を負う。

c. データ・プロセッサーである IBM およびそのサブプロセッサーにお客様の「個人データ」の処理を許可するために必要なデータ処理契約をコントローラーと締結する。

d. IBM の単一の連絡窓口として機能し、IBM に対するその他のコントローラーであるお客様の「関連会社」の指示または要求の内部調整、確認および提出について全責任を負う。IBM は、かかる情報または通知をお客様に提供したときに、コントローラーとなるお客様の「関連会社」に知らせるか、通知する義務から解放されるものとします。IBM は、お客様ではないコントローラーになるお客様の「関連会社」によって直接提供された指示を拒否する資格があります。

いずれの当事者も、かかる当事者の「適用可能なデータ法」に違反して行動することは求められないものとします。

8.2 お客様のデータに関する権利

お客様は、(a) 自らが「IBM SaaS」に入力するデータを所有すること、または (b) 本 ToU もしくは本契約に規定されている条件に従って、または IBM が「IBM SaaS」を提供するのに必要なその他の方法に従って、「お客様データ」へアクセスし、使用し、開示する権利を IBM に付与するために必要なすべての権利、許可、同意および権限を取得ずみであり、それらを維持することに責任を負っていることを表明し、保証します。お客様は、「お客様データ」が (a) 米国に居住する個人に関係するもので、米国のデータ・センターでのみ「IBM SaaS」に入力されるものであるか、または (b) 1 つ以上の「対象国」に居住する個人に関係するもので、「指定データ・センター」でのみ「IBM SaaS」に入力されるもののいずれかであることをさらに表明し、保証します。

8.3 データに関するサービスおよび責任

a. お客様は、お客様の「医療業務」または「調査」(それぞれ、HIPAA またはお客様が使用する「適用可能なデータ法」の定義どおり) のいずれかに該当する活動に関連して、「お客様データ」の分析を実行するか、IBM に分析を実行するよう要求すること、およびこれらおよびその他の「お客様の適用可能なデータ法」に基づくすべての関連する要件 (例: 地域により「倫理審査委員会」の判断または権利放棄) に従って、お客様が「お客様データ」を使用するか、 IBM に「お客様データ」を使用するよう指示することに同意します。

b. お客様は、お客様ならびに IBM および IBM が許可した従契約者が本 ToU および本契約に基づいて意図されたとおりに「お客様データ」を「IBM SaaS」に入力し、使用し、開示するために、該当する各「対象国」においてお客様の「適用法」 (HIPAA およびその他の該当するデータ・プライバシーおよびセキュリティーに関する法律、規則、および規制が含まれますが、これらに限定されません。) により要求されるあらゆる登録、同意、権限、および許可を取得する全責任を負います。IBM は、かかる登録、同意、権限および許可がいつ受理または要求されたのかを監視する責任は一切負わないものとします。

c. お客様は、「IBM SaaS」に入力されたお客様のすべての「データ」が米国または該当する「対象国」に居住する個人に関連するデータに制限されることを徹底させる全責任を負います。

d. IBM は、「対象国」からのデータに関して、HIPAA およびその他の「IBM の適用可能なデータ法」について研修を受けた担当者のいるサポート・センターを備えているものとします。

8.4 セキュリティー対策およびセキュリティー・インシデント

a. IBM は、技術対策および組織対策 (組織的なプロセスや手順を含む、ならびに本 ToU および SBCA に規定されるか、本 ToU および SBCA で言及される特定のセキュリティー義務を含みます。) を導入、維持および遵守して、お客様の「個人データ」を不正使用もしくはアクセス、偶発的な損失、損害、変更、破棄、盗難または不正開示から保護します。

b. IBM がお客様の「処理済みデータ」が関与している「セキュリティー・インシデント」(SBCA の定義どおり) に気が付いた場合、IBM は、SBCA および「IBM の適用可能なデータ法」に従ってお客様に通知するものとします。また、かかる通知には、お客様、またはかかる「セキュリティー・インシデント」の影響を受ける「データ主体」(該当するものがある場合) に対する既知の影響、ならびに IBM が講じた、もしくは講じることを提案した是正措置が記載されます。

8.5 問い合わせおよび苦情の受理

IBM は、「IBM の適用可能なデータ法」で認められる限りにおいて、IBM が以下から受理した、お客様の「個人データ」に関する問い合わせ、コミュニケーションまたは苦情を IBM Watson Health Data Privacy Officer が受理後 5 日以内に、書面にて速やかにお客様に通知するものとします。

a. 「データ主体」(IBM が処理したかかる「データ主体」についての「個人データ」に関連)。お客様は、「データ主体」からのかかる要求に対応するものとし、IBM はお客様がかかる要求に対応する際の支援に関してお客様の相応の指示を遵守します。IBM の「適用法」で要求されている場合、IBM はかかる要求に直接対応できます。ただし、IBM の「適用法」で認められている場合、もしくはその他の方法で可能な場合、IBM が事前にかかる対応をお客様に通知し、かかる対応の形式や内容についてお客様と相応に調整することを条件とします。

b. 法律関連または規制関連の当局 (お客様の「個人データ」の IBM による「処理」に関連)。ただし、IBM による開示を強制する (法律で認められている場合、もしくはその他の方法で可能な場合、IBM がかかる開示についてお客様に通知し、かかる対応の形式や内容についてお客様と相応に調整することを条件とします。)、または「適用可能なデータ法」によりその他の方法で要求される召喚状もしくは類似の法律文書により、IBM が、政府機関から受理したかかる要求に対応できることを条件とします。

8.6 お客様の個人データの処理

IBM は、お客様の「個人データ」の開示を、「サービス」を提供する際に支援を必要とする可能性のある「IBM 担当者」に制限するものとします。

IBM は、「適用法」に従ってお客様の「個人データ」を変更、修正、削除またはブロックするよう IBM に要求する、お客様からの相応の要求を遵守するものとします。

いずれかの当事者の要請を受けて、IBM、お客様またはそれぞれの「関連会社」は、お客様の「個人データ」の保護のために法律で要求される標準の契約を締結します。両当事者は、両当事者間の申告目的で、かかる契約に本契約の責任の制限および免責が適用されることに同意 (し、それぞれの「関連会社」に同意させるように) します。両当事者は、「適用可能なデータ法」で要求されるとおりに、さらに相互に合意した条件または契約を締結 (するか、かかる「当事者」の「関連会社」に締結させるように) して、遵守する際に協力するものとします。

8.7 お客様の個人データの返却

本契約の満了または終了と同時に、IBM は、お客様の「専有情報」およびお客様の「個人データ」の使用および処理を中止するものとし、またすべての「IBM 担当者」に同様に中止させるものとします。さらに、お客様のオプションおよび要求により、以下を行うものとします。

a. お客様が相応に要求できる形式およびストレージ・メディアで、IBM が電子的に保管しているすべてのお客様の「専有情報」およびお客様の「個人データ」を速やかに返却し、お客様の受け取り確認を受けて、当該のお客様の「専有情報」およびお客様の「個人情報」(コピーおよびバックアップを含みます。) を削除するか、破棄するか、またはその他の方法で永続的に読み込み不可にするか、判読不可にする。IBM は、ストレージ・メディアの費用、およびお客様の要求に基づき実施した特定の活動 (指定の形式でお客様の「専有情報」およびお客様の「個人データ」を提供する、またはお客様の「専有情報」およびお客様の「個人データ」を特定の方法で破棄するなど) に対する料金を請求することができます。

b. 当該のお客様の「専有情報」およびお客様の「個人情報」(コピーおよびバックアップを含みます。) を直接削除するか、破棄するか、またはその他の方法で永続的に読み込み不可にするか、判読不可にする。

8.8 ビジネス・アソシエート契約

適切かつ HIPAA で要求される限りにおいて、IBM およびお客様は「ビジネス・アソシエート契約」(以下「BAA」といいます。) を締結します。これは、「IBM SaaS」の提供においてお客様の「ビジネス・アソシエート」である IBM の義務に適用されるものとします。本契約に基づく、および BAA がある場合にはそれに基づく IBM の明確な義務を制限することなく、お客様は、「IBM SaaS」に関するお客様の使用またはその他の活動 (「許可ユーザー」による使用またはその他の活動を含みます。) に適用される、すべての「適用法」およびライセンス交付要件の可用性を判断して、それらを遵守する責任を負うことを了承し、それに同意します。

8.9 EU のデータ処理に関する補足契約

お客様が IBM に EU の「個人データ」を処理するよう指示する場合、IBM およびお客様は、オプション条項を省いた、場合に応じて EU 標準契約条項を含む、「データ処理に関する補足契約」を締結します。

9. 「IBM SaaS」オファリングの追加条件

9.1 セキュリティー

本「IBM SaaS」は、IBM の「IBM SaaS」に関する「Data Security and Privacy Principles」(http://www.ibm.com/cloud/data-security で入手可能)、ならびに以下に規定される、および本 ToU の「セキュリティーおよび事業継続性に関する別紙」に規定される、追加条件に従います。IBM の「IBM SaaS」に関する「Data Security and Privacy Principles」が変更される場合であっても、それにより「IBM SaaS」のセキュリティーのレベルが低下することはありません。

IBM Watson Health Core は、「セキュリティー記述書」にさらに詳しく記載される ISO 27001 の枠組みに基づいてセキュリティー・ポリシー、標準、およびプロセスを実装します。セキュリティー機能のうち、このソリューションは以下を実装します。

a. セキュアなオペレーティング・ゾーン

   IBM Watson Health Core は、奥行きのある戦略に保護を実装し、複数のセキュリティー・ゾーンを利用して、データ・オンボーディングおよびカスタム・アプリケーション開発といったクラウド統合ポイントを管理します。

b. 暗号化

   すべての「お客様データ」は保存中も処理中も暗号化されます。IBM Watson Health Core を転送先および転送元とする転送中のすべてのデータは暗号化されます。共有サービスでは暗号化鍵管理が提供されます。お客様は、IBM Watson Health Service とお客様のプロキシー・サーバー間のすべてのネットワーク接続および品質について責任を負います。

c. セキュリティー・イベント・モニタリング

IBM は、自社のセキュリティー・インテリジェンス・プラットフォームを活用して、セキュリティー情報およびイベント管理、ログ管理、インシデント・フォレンジック、脅威検出および脆弱性管理に対応します。

d. アイデンティティ管理

- Watson Health Core は、OpenID Connect を使用して大規模な患者およびユーザーの各母集団に対応するオープン・スタンダード ID プロバイダーをサポートします。
- IBM が ID プロバイダーを務めるユーザーの母集団について、Watson Health Core は適切なディレクトリー・サービスおよび ID 管理機能を活用して認証を処理します。

e. 強力な認証および役割ベースのアクセス

- Watson Health Core は、お客様がそれぞれの「シングル・サインオン (SSO)」またはディレクトリー・サービスを統合するための仕組みである SAML を通じて認証をサポートします。
- Watson Health Core はアクセス管理ソリューションおよび関連コンポーネントを活用して、必要に応じてセキュリティー・ポリシーを管理します。
- Watson Health Core は、ソフトウェア・ベースの 2 要素認証をサポートします。
- Watson Health Core は、必要に応じて、基本的な役割ベースのアクセス制御を提供します。Watson Health Core は、役割ベースのアクセスを可能にするプログラム・アプリケーション・プログラミング・インターフェース (以下「API」といいます。) を通じて、調査、ユーザー・プロファイル、役割、およびユーザー・グループの構成をサポートします。

9.2 Cookie

お客様は、IBM が「IBM SaaS」の通常の運用およびサポートの一環として、トラッキングおよびその他の技術により、「IBM SaaS」の利用に関連してお客様 (お客様の従業員および従契約者) から個人情報を収集することがあることを認識し、これに同意するものとします。IBM によるこのような情報収集は、ユーザー・エクスペリエンスの向上またはお客様との対話の調整を目的とし、「IBM SaaS」の有効性について使用統計および情報を収集するために行うものです。お客様は、IBM、その他の IBM グループ会社およびその従契約者が、営業活動を行う地域において、適用法に従い、IBM、その他の IBM グループ会社およびそれぞれの従契約者の範囲内で、収集した個人情報を前述の目的のために処理することができるよう、お客様が同意を取得すること、または取得済みであることを確認するものとします。IBM は、収集した個人情報へのアクセス、更新、修正または削除について、お客様の従業員および従契約者からの要求に従うものとします。

9.3 Derived Benefit Locations

該当する場合、お客様が「IBM SaaS」に関する利益を享受しているとお客様が特定する所在地の税金が適用されます。IBM は、お客様が IBM に追加情報を提供する場合を除き、「IBM SaaS」の注文時に主要な Benefit Location として記載した事業所住所に基づいて税金を適用します。お客様は、当該情報を最新状態に保ち、変更があった場合には IBM に通知する責任を負うものとします。

9.4 継続的デリバリー

お客様は、ソリューションに合わせて作成され、IBM によって継続的なクラウド・デリバリー・モデルに導入される機能および拡張機能を使用する資格があります。

9.5 バックアップおよびリストア

IBM Watson Health Core は、システム障害に備えてサービスを復旧する目的で、確認されている最新の良好な状態について、実稼働環境で「お客様データ」のバックアップ (Data Lake および Data Reservoir の各リポジトリーを含みます。) を提供します。

9.6 高可用性

実稼働環境における IBM Watson Health Core コンポーネントは、ワークロードを分散し、単一障害点を排除するために、冗長性に対応してクラスター化されたデータベース・サーバーにより、高可用性の構成に実装されます。

9.7 災害復旧

IBM の災害復旧のアプローチは、「実稼働」環境向けの以下の事業継続性目的を達成することを目的とする分散地域にある複数のデータ・センターで構成されています。

- RTO – 災害宣言から 36 時間以内
- RPO – お客様のコンテンツの喪失から 24 時間以内

9.8 計測ツール

「IBM SaaS」は、合成モニタリング・ソリューションを使用して、コミットされたサービス・レベルに照らして、可用性または障害について監視、測定および報告を行います。このソリューションは、グローバル・レベルでユーザー応答およびユーザー・エクスペリエンスをシミュレートして追跡します (静的可用性および取引の両面について)。

「IBM SaaS」は、ソリューション全体にわたるメトリック、イベント、およびアラートに対応するために内部モニタリング・システムも使用します。

9.9 広報活動

お客様は、IBM が広報活動またはマーケティングのコミュニケーションにおいて、お客様のことを「IBM SaaS」のサブスクライバーとして公に言及できることに同意します。

別紙 A

1. IBM Watson Health Core

IBM Watson Health Core は、IBM が所有または管理するデータ・センターに配置された、HIPAA で定義されている「保護医療情報 (PHI) 」および「IBM の適用可能なデータ法」に準じたその他の「ヘルス・データ」の保管、キュレーション、および処理を行うための、「ヘルス・データ対応」の Platform as a Service (PaaS)、開発プラットフォーム、および運用サブシステムです。お客様は、下記のフィーチャーおよび機能を有効化するためには、IBM Watson Health Core および IBM Watson Health Core Access に対する適切な使用許諾を取得しなければなりません。

1.1 Watson Health Core 稼働環境

Watson Health Core 使用許諾には、お客様が「ヘルス・データ」を処理できるように設計された、3 つの「ヘルス・データ対応」クラウド稼働環境が含まれます。

- パイロット

  お客様が「IBM SaaS」を使用して構築されたアプリケーションを開発してテストできる場所となる、サンドボックス環境を提供します。このパイロット環境は、システム・オブ・レコードの「災害復旧」、高可用性およびバックアップを除き、HIPAA セキュリティー制御をすべて実装します。

- 実稼働環境

  お客様が「ヘルス・データ」ワークロードを導入できる場所となる実寸大の環境を提供します。実稼働環境は高可用性のロード・バランス化された環境で、「災害復旧」ロケーションへフェイルオーバーできます。

- 災害復旧

  「実稼働」環境のミラー・レプリカを提供します。別個のデータ・センター・ロケーションに配置されます。

1.2 アプリケーション開発

IBM Watson Health Core は、アプリケーション開発、およびお客様のデバイスまたはお客様の許可ユーザーのデバイスからの安全なデータ収集を可能にします。API は、お客様の許可ユーザー (お客様の第三者サービス・プロバイダーを含みます。) がアプリケーションを開発したり、「IBM SaaS」とデータを交換したりするために使用できるプログラム・インターフェースおよび資料を提供します。お客様およびその開発者による API の使用は、「API 開発者要件」の遵守が条件となります。

- REST API

  Watson Health Core は、Watson Health Core プラットフォーム向けの一連の REST API およびサービスを提供します。API 機能には、データ・リポジトリー、データ・キュレーション・サービス、ユーザー管理、および監査ログへアクセスするための仕組みが含まれますが、これらに限定されません。

- Apple HealthKit および Apple ResearchKit

  Watson Health Core は、iOS ベースの調査研究向けの Apple ResearchKit API フレームワークおよびヘルス・データを取り込むための Apple HealthKit との統合をサポートします。

1.3 データ・ガバナンス

- 同意管理

  Watson Health Core は、患者または調査参加者から提供された同意を取り込むための枠組みを提供し、同意に対応したお客様アプリケーション経由で個人が登録する際のデータ・ペイロードと分けて、同意の記録を安全に保管できます。

- データ・マスキング

  Watson Health Core は、名前の ID を構造化データのペイロードと分ける能力を提供します。Watson Health Core はプログラム API を通じてクラウドでデータを受信します。API は、別個の暗号化されたデータ・ストアに保管される、患者または個人の名前の ID を、そのデータ・ペイロードの残りの部分から切り離せるようにします。データ・ペイロードには、将来の出所追跡に使用できる匿名トークンが割り当てられます。

1.4 ヘルス・データ・サービス

Watson Health Core は、外因性の「ヘルス・データ」およびその他の「個人情報」を含むデータ (構造化および非構造化の両方) の収集、保管、同期を提供します。

- データの取り込み

  Watson Health Core は、プログラム API を通じて患者のアプリケーションまたはデバイスからデータを取り込む能力を提供します。Watson Health Core は、お客様の「権限を有する個体」のそれぞれに、契約期間の各年につき、最大 25 MB のデータを Health Core にアップロードする資格を付与します。このサービスは、1 日当たり「個体」につき最大 10 のアップロードに対応します。

- 運用上の Data Lake

  未加工のお客様データまたは患者データは、分析やモデル化のために必要とされるまで、ネイティブに Watson Health Core で保管されます。

- Extract Transform Load (ETL)

  データはオペレーション・サブシステム内で正規化フォーマットに変換されます。医療施設の業界標準ベースの「エンタープライズ・サービス・バス」は、さまざまなお客様アプリケーション間およびプロトコル間の統合を可能にします。

- Data Reservoir

  キュレーションされたデータは Data Reservoir に移されます。Watson Health Core は IBM Unified Data Model for Healthcare の側面を使用し、ビジネスおよびテクニカルのヘルス・データを正規化して分析で使用します。

- マスター患者インデックス

  Watson Health は、複数のリソースからのデータを統合するために「マスター・データ管理」ツールを提供して、「縦断患者記録 (LPR)」を作成します。

2. オプション機能

2.1 IBM Watson Health Core Terminology Service

このアドオン・サービスにより、異なる医療システム間のデータ統合と相互運用性を促進して、すべての Watson Health Cloud アプリケーションにわたって一貫性のある臨床用語の使用を提供します。このサービスは、以下のような、用語、コード・システム、および構造化コンテンツを含むタスクに対応した機能プラットフォームを提供します。

- 新規コード・システムの作成。
- 国際コード・システムの変換。
- ローカル・コード・リスト間および国際標準間のマッピング。

別紙 B

IBM は、「PoE」に記載するとおり、「IBM SaaS」に関して、以下の可用性のサービス・レベル・アグリーメント (以下「SLA」といいます。) を提供します。「SLA」は保証ではありません。「SLA」はお客様にのみ提供され、実稼働環境における使用に対してのみ適用されます。

1. 可用性クレジット

可用性のリベートは、「個体」の使用許諾に対するサブスクリプション料金に対してのみ適用可能です。

お客様は、「IBM SaaS」の可用性に影響を及ぼした事象について最初に知り得たときから 24 時間以内に、IBM テクニカル・サポート・ヘルプデスクに対して「重要度 1」のサポート・チケットを記録しなければなりません。お客様は、あらゆる問題診断および解決に関して IBM を合理的な範囲で支援しなければなりません。

「SLA」の未達を申告するサポート・チケットは、契約月の末日から 3 営業日以内に提出しなければなりません。有効な「SLA」の申告に対する補償は、「IBM SaaS」の実稼働システム処理が利用できない時間 (以下「ダウンタイム」といいます。) に基づいた「IBM SaaS」の将来の請求に対するクレジットになります。「ダウンタイム」は、お客様が当該事象を報告した時点から「IBM SaaS」が復元される時点までの間で計測され、次のものに関連する時間は含まれません。保守のための計画停止または発表された停止、IBM の支配の及ばない原因、お客様または第三者のコンテンツもしくはテクノロジーの問題または設計もしくは指示、サポート対象外のシステム構成およびプラットフォームまたはその他お客様による誤り、またはお客様に起因するセキュリティーに関する事故もしくはお客様によるセキュリティー・テスト。IBM は、下表のとおり、各契約月における「IBM SaaS」の累積的な可用性に基づき、適用しうる最大の補償を適用します。各契約月の補償の合計額は、「IBM SaaS」に対する年額料金の 12 分の 1 の 20% を超えないものとします。

2. サービス・レベル

「契約月」における「IBM SaaS」の可用性

「契約月」における可用性	**補償 (申告の対象である「契約月」における 「月額の「個体」サブスクリプション料金」* の割合)**
< 99.95%	10%
<99.0%	20%

*「IBM SaaS」が IBM ビジネス・パートナーから取得されたものである場合、月額サブスクリプション料金は、申告の対象である「契約月」に対して有効な「IBM SaaS」のその時点での最新の表示価格に基づいて計算され、それを 50% 割引した額となります。IBM は、直接お客様に払い戻します。

「可用性」は、以下のとおり算出されます。契約月における分単位の総時間数から、契約月における「ダウンタイム」の分単位の総時間数を差し引き、それを契約月における分単位の総時間数で除することにより算出され、結果はパーセントで表します。

例:「契約月」における「ダウンタイム」が 108 分である場合

30 日の「契約月」における合計 43,200 分
-「ダウンタイム」108 分
= 43,092 分
———————————————
合計 43,200 分

=「契約月」における 99.75% の可用性につき
10 % の「可用性クレジット」

3. 除外事項

本「SLA」は、以下の場合には適用されません。

- サーバー・モニタリングは別として、SLA は、カスタム・アプリケーションまたはお客様アプリケーションをサポートすることを目的として、ホスト仮想マシンに適用されることはありません。
- お客様が、現行の契約上の義務に基づいた重要な義務に違反した場合。

別紙 C

この「セキュリティーおよび事業継続性に関する特則 (以下「本 SBCA」といいます。)」では、IBM が「IBM SaaS」をお客様に提供する上での IBM の一定の要件と義務を規定しています。本書に定める要件と義務は、「IBM SaaS」のデータ・セキュリティーに関する原則の説明書 (http://www.ibm.com/cloud/data-security で入手可能) に規定されている要件と義務に追加されるものです。本書に定義されていない鍵括弧つきの用語は、本契約または利用条件に定める意味を有するものとします。

1. 機密保護プログラム

IBM には、ISO 27001 の枠組みと統制領域に基づく社内のセキュリティーに関するポリシー、標準、およびプロセスがあります。IBM の企業セキュリティー組織のガバナンスに加えて、これらのポリシー、標準、およびプロセスは、定期的に内部監査の対象となります。

IBM では、お客様コンテンツの処理、保管および伝送に適用される、組織面、運用面、管理面における、物理的および技術的な安全対策の機密保護プログラムを維持しており、これは最低限、本 SBCA の要件に整合したものです。

IBM は、お客様の要求に応じて、お客様がその継続的な適合性、妥当性および有効性を合理的に判断できるよう、IBM Watson Health の機密保護プログラムに関する情報をお客様と共有するものとします。IBM Watson Health の機密保護プログラムは、一般に受け入れられている業界の慣行および IBM の「適用法」の変化に対応するため、随時更新されるものとします。

2. アクセス制御

IBM は、お客様コンテンツについて、IBM がその義務をお客様に対して遂行する支援を行うためにかかるお客様コンテンツにアクセスする正当な業務上のニーズを有する自社の従業員、従契約者もしくは第三者、または「適用法」、本契約もしくは「関連文書」(該当するもの) に従って、「IBM SaaS」を提供するために必要なその他の個人にのみ、開示するものとします。IBM がお客様の「ビジネス・アソシエート」である場合は、IBM とお客様は、両当事者間における該当する「ビジネス・アソシエート契約」の条項に従ってのみ、「個人医療情報」を開示するものとします。

IBM には、正式な、社内のユーザー・アクセス管理プロセスがあり、それにより、ユーザーのアクセスが正式に要求され、本人確認の上で承認され、最小特権の概念を用いて、知る必要に基づいて権限付与されます。お客様コンテンツへのアクセスは、アクティブ・ユーザーおよびアクティブ・ユーザー・アカウントのみに制限されるものとします。IBM には、アクティブ・ユーザー・アカウントの、定期的社内アクセス権限再確認のための、正式なプロセスがあります。

IBM では、セキュアなユーザー認証プロトコルを使用しており、これには、IBM の企業セキュリティー基準およびポリシーに従った、お客様へのサービス提供に使われるシステム上での固有の識別番号と強力なパスワードの割り当てが含まれます。

a. パスワードは、ベンダーから提供されたデフォルトのパスワードであってはならず、保護対象のデータのセキュリティーを危殆化しない場所に、そのようなフォーマットで保管されるものとします。

b. パスワードの表示や印刷を行う場合は、権限のない第三者が看取したりその後に復旧したりできないように、マスキング、表示抑制等の方法で覆い隠す必要があります。パスワードは、入力中に記録したり、取り込んだりしてはなりません。ユーザー・パスワードは、平文で保管してはなりません。

c. 「IBM SaaS」を構成する各テクノロジー用のパスワードは、既知のパスワード長さの脆弱性に関連するリスクを軽減するべく選択され、文書化される必要があります。

d. 運用上の理由で社内の、特権化された、共有の職能別 ID が必要な場合、IBM は、共有の、職能別、または「システム ID」を、個人の責任を維持するために、パスワードのチェックアウトを要求して管理します。

非アクティブ・タイムアウトが、お客様コンテンツを格納するすべてのシステムとアプリケーションに対して設定されます。

必要であれば、お客様コンテンツを格納する IBM のネットワーク、システムおよびアプリケーションへのリモート・アクセスが、お客様の要求と IBM の正式な承認に基づいて設定されるものとし、すべてのかかるリモート接続は、強力な認証と暗号化のプロトコルを用いて保護されるものとします。リモート・アクセスのアクティビティーは、記録や監視の対象となるものとします。

「IBM SaaS」の提供において、IBM がお客様の社内ネットワーク内の何らかのシステムにリモートでアクセスする必要がある場合、すべてのかかるリモート・アクセスは、お客様のセキュアなリモート・アクセスのシステムとプロトコルを使って、かつお客様から IBM に提供されたアクセス資格情報を用いて実行されます。お客様のネットワークへのリモート・アクセスは、IBM による要求とお客様による承認があった場合にのみ、かつ事前に IBM に提供される、お客様のその時点で最新のポリシーに従って、確立されます。IBM によるお客様の社内ネットワークの使用には、事前に IBM に提供される、お客様の IT 利用およびセキュリティーに関するポリシーが適用されます。

IBM では、セキュリティー管理、アクセス・レビュー、およびセキュリティー違反について、職務分掌を実施しています。

お客様に固有のお客様コンテンツの保管、ホスティングおよび処理は、IBM がサービスを提供する他のお客様のものから、論理的に分離されます。共有のストレージ、ホスティングまたは処理の作業域がお客様により許可されている場合、IBM は、当該お客様コンテンツの不正な開示を防止するべく作られた、本 SBCA に規定する要件と整合した手順および安全対策を有しているものとします。

IBM では、お客様コンテンツがいかなる時も公共の場に無人の状態で置かれることがないようにするための、クリーン・デスク/画面消去のポリシーを導入しています。

3. 転送と暗号化

IBM は、お客様コンテンツの送信 (ファックス、電子メール、クーリエ便などによる) において、受領者について正確な連絡先情報が使用されるようにし、当該情報の受領を安全で確実なものとするために、目的とする受領者と事前の取り決めを行うことで、適切な予防措置をとるものとします。

IBM は、お客様コンテンツの処理に関連して、常時適切な形式の暗号化もしくはその他の安全対策テクノロジーを使用するとともに、「IBM 担当者」にも使用させます。これには、お客様コンテンツの転送、伝達、リモート・アクセスまたは保管 (バックアップ保管を含みます。) に関連する処理が含まれます。たとえば、IBM は、次のようなお客様コンテンツが含まれるすべてのレコードとファイルを、適切な業界標準の暗号化を用いて暗号化するものとします。

a. オフサイトの保管設備への移送の際に、IBM のラップトップ、ポータブル・デバイスまたはポータブル電子メディア (バックアップ・テープなど) に格納されたもの
b. お客様のまたは IBM の物理的に保護されたオフィスや施設の外部で IBM により格納または移送されたもの (ハードコピーの紙文書は除く)
c. IBM による公衆ネットワーク間の移動中に
d. IBM のシステムからお客様への転送中に
e. IBM によるワイヤレス送信中に
f. IBM によりサーバーやデータベースに格納されたもの

4. ネットワーク・セキュリティー

IBM は、ファイアウォール、プロキシ、Web アプリケーション・ファイアウォールおよびインターフェースなどの、合理的に最新版のシステム・セキュリティー・ソフトウェアを使用しています。かかるソフトウェアには、マルウェア保護対策ならびに合理的に最新のパッチおよびウィルス定義が含まれている必要があります。事業者基準に従って、技術的に可能な場合はワークステーション、サーバーおよび関連エンドポイントにアンチウィルス・ソフトウェアがインストールされるものとし、当該ソフトウェアは、社内管理ソリューションで企業ポリシーに沿って管理されます。

IBM では、セキュリティー・インシデントを可能な限り速やかに検知して特定するために、「IBM SaaS」を監視しています。IBM は、最低限、業界標準の侵入検知ツールならびに予防、監視および対応プロセ

スを、お客様コンテンツまたはお客様へのサービス提供に使用されるシステムの不正な開示、濫用、改変、もしくは破壊につながりうる、社内外の脆弱性やリスクを特定するべく企図された方法で、維持するものとします。

IBM は、脆弱性に関する情報サービスまたは機密保護に関する助言サービスおよびシステムの脆弱性に関する現行情報を提供するその他の関連ソースに加入しています。IBM は、定期的な脆弱性影響評価および自身のネットワークの修復を実施しています。

IBM は、「セキュリティー・インシデント」を検知、特定、阻止、および解決するために、「IBM SaaS」を監視しています。

IBM は、IBM リリース管理プロセスを通じて、「IBM SaaS」が提供されているネットワーク・セキュリティー・インフラストラクチャーの可用性、完全性および有効性を検証しています。

5. インシデントの管理および通知

IBM Watson Health チームは、IBM のオファリングに関連するセキュリティー・インシデントの受領、調査および調整を管理するグローバル・チームである IBM Cybersecurity Incident Response Team と連携して、ソフトウェア関連のセキュリティー問題を減らすために必要な予防手段を導入しています。「セキュリティー・インシデント」とは、システム操作または「IBM SaaS」の提供のために IBM が使用する情報システム内のデータへの無許可のアクセス、使用、開示、変更、または妨害です。「セキュリティー・インシデント」が (ルーチンのスキャン操作、アラート、しきい値イベントなどで) 発見された場合、IBM はお客様に以下を通知します。

a. お客様コンテンツに伴う「セキュリティー・インシデント」を、可及的速やかにかついかなる場合も、当該「セキュリティー・インシデント」の調査および確認後 2 営業日以内に

b. 政府関係者 (データ保護機関や法執行機関を含む) からの、お客様コンテンツへのアクセスまたはそれに関する情報の要求を受けた場合、速やかに (法律または関連の命令によりそれが禁止される場合を除く)

c. 本 SBCA の「アクセス制御」と題されたセクションで許される場合を除き、第三者へのまたは第三者によるお客様コンテンツの開示もしくは転送、またはアクセスが行われる場合に事前に

6. ロギング

IBM は、IBM のポリシーおよび慣行ならびに一般に受け入れられている業界慣行に従って、お客様の「処理済みデータ」の無許可のアクセスまたは使用に対する、システムの合理的な監視を実施しています。実際のまたは試みられたログオン違反およびアクセス違反を、ログに記録するものとします。

IBM は、お客様のデータおよび「ヘルス・データ」の保管、アクセス、処理および伝送を行うすべてのシステムに対する、すべてのアクセス要求およびアクセス操作のログを、HIPAA およびその他の「IBM の適用可能なデータ法」で要求される期間、維持します。

このログおよびレポートには、少なくとも以下が含まれます。(i) 合理的な識別情報を含む、すべてのログイン試行 (成功か不成功かを問わない)、(ii) アプリケーションのインストール、ユーザー管理の変更、およびファイル・アクセス権の変更を含む、すべてのシステムおよびネットワーク構成の変更、(iii) ファイル、ネットワーク・シェア、ログ、またはその他のリソースへのアクセスの試行を含む、リソースへのアクセス試行 (成功か不成功かを問わない)、ならびに (iv) データのダウンロード (データのコンテンツ・タイプおよびダウンロードの達成に用いられたアクセス・プロトコルを含む)。

7. ソフトウェア・アプリケーション開発および変更管理

IBM は、実稼働アプリケーションおよび関連ソース・コードの完全性を無許可かつ未テストの修正から保護する、セキュアなアプリケーション開発およびコーディングの慣行に従います。

IBM は、以下を含む変更管理プロセスに従います。(a) 変更内容の記録と正式な承認、ならびにバックアウト手順、ならびに (b) ユーザー受け入れテスト (該当する場合)、およびセキュリティーのテストを含む、当該変更の適切なテスト。

IBM は、お客様コンテンツの保管、アクセスおよび伝送に使用される、または「IBM SaaS」などのサービスをお客様に提供するために使用されるすべてのシステムへのインストールに先立つパッチのテストを含む、パッチ管理プロセスに従います。

IBM は、お客様コンテンツの保管、アクセスおよび伝送に使用されるすべての情報システムの構成に関する、完全で、正確な、かつ最新の情報を維持するよう、システム管理者に義務付けます。

8. 物理的および環境上のセキュリティー

IBM Watson Health Core のプラットフォームは、IBM SoftLayer のデータ・インフラストラクチャー上に導入されます。IBM SoftLayer は、人的な、環境による、および技術的な違反や影響からお客様データを保護するための、物理的および環境面のセキュリティー、アクセス制御、コントロールおよびプロセスを備えています。

「IBM SaaS」がホストされる設備への一般アクセスは、カード・アクセス・システムの利用によって管理されています。閉回路テレビ (CCTV) カメラが、サイト全体に設置され、保安要員により監視されています。入退室専用扉にはアラームが設置され、保安要員がこのアラームを監視しています。

管理区域への立ち入りは、カード・アクセスおよび/または追加の生体認証の利用により制限されています。管理区域へのアクセス権限を持たないすべての個人は、サインインを行い、承認された管理区域へのアクセス権限を持つ個人に同伴してもらう必要があります。管理区域の全非常口には、音響アラームが設置され、保安要員がこのアラームを監視しています。アラームが正しく機能することの定期的な確認が実行され、文書化されて保持されます。管理区域へのアクセス権は、四半期ごとに完全な再検証が行われます。管理区域へのアクセス権は、雇用の終了時に取り消されます。

施設は、火災報知器、消火設備、煙探知器、ならびに防火・消火システムを通じて火災や水害、熱などの環境要因から保護されています。施設は、無停電電源装置 (UPS) システムおよび補助発電機により、停電から保護されていて、これらは定期的に保守とテストが行われています。

IBM SoftLayer に関するコンプライアンス情報とレポートは、http://www.softlayer.com/compliance で確認できます。

9. 事業の継続性

IBM には、本契約に基づくその義務に合致したサービス・レベルを維持するべく企図された、事業継続性および災害復旧の計画があります。かかる事業継続性および災害復旧の計画は、定期的に (少なくとも年 1 回) 更新され、テストされるものとします。IBM は、一般に受け入れられている業界慣行に準拠し続けるために必要な、事業継続性および災害復旧の計画に対するすべての合理的な変更を実施するものとし、それぞれの場合において、お客様により使用されている「IBM SaaS」や実稼働環境を不当に妨害しないものとします。

お客様が「IBM SaaS」を利用できなくなるような災害が発生した場合、IBM は速やかにお客様に通知するとともに、事業継続性計画および/または災害復旧計画を発動するものとします。災害が宣言された場合、「IBM SaaS」の事業継続性の目標は、次の通りお客様による「IBM SaaS」へのアクセスを復元することです。停止の場合、IBM Watson Health の実稼働環境の「目標復旧時間 (RTO)」は、災害宣言から 36 時間以内となります。「目標復旧時点 (RPO)」は、実稼働環境内のお客様のコンテンツの喪失から 24 時間以内となります。具体的な Watson Health ソリューションの事業継続性目標は、異なる場合があります。

災害復旧に対する IBM のアプローチは、分散した地理上の区域における複数のデータ・センターからなります。

すべての IBM SoftLayer データ・センターでは、複数の電源供給、ファイバー・リンク、専用発電機、およびバッテリー・バックアップを備えています。これらは業界最高レベルのハードウェアと機器で構築されており、最高水準の性能、信頼性、および相互運用性を提供します。データ・センターのコンポーネントはすべて (たとえば予備の n+1 電源および冷却装置など)、データ・センター内での安定度を維持するよう、検査されています。

10. 遵守

IBM のセキュリティー・プラクティスは、ISO 27001-27002 に基づいています。これらのプラクティスは、「リスク分析」、「物理的セキュリティー」、「緊急時計画」、「調査」、「情報保護」、「教育」、「データ保護」、および「運用」(ただしこれらに限りません。) に関する統制体制を備えています。

IBM は、IBM のセキュリティー・プラクティスの遵守に関して、セキュリティーおよびプライバシー関連のアクティビティーをレビューします。

IBM は、「対象管轄区」における「IBM の適用可能なデータ法」を遵守します。

お客様の機密情報の適切な取り扱いも、IBM の「ビジネス・コンダクト・ガイドライン」に基づいて義務付けられています。このガイドラインは、全従業員が年に 1 回レビュー (し、そのレビューを認定) する必要があります。

11. その他

IBM は、「IBM SaaS」の提供に携わるすべての従契約者および第三者との契約、ならびに該当する「関連文書」に、本 SBCA におけるものと最低限同等にお客様コンテンツを保護する条件が確実に盛り込まれるようにします (それぞれ、当該の従契約者や第三者により履行されるサービスにかかる条件が適用される場合)。